BEZPEČNOSTNÝ BULLETIN

Týždeň 09. 12. 2020 - 15. 12. 2020

OBSAH BEZPEČNOSTNÉHO BULLETINU

Č.	Identifikátor	Dôležitosť	CVSS Skóre
01.	Viacero zraniteľností v produktoch Microsoft	Vysoká	**8.8**
02.	Zraniteľnosti v Medtronic MyCareLink Smart Model 2500 Patient Reader	Vysoká	**8.8**
03.	Zraniteľnosti v platobných termináloch Verifone a Ingenico Telium	Vysoká	**8.8**
04.	Viacero zraniteľností v portfóliu produktov Siemens	Vysoká	**8.1**
05.	Zraniteľnosti vo WECON LeviStudioU	Vysoká	**7.8**
06.	Zraniteľnosť v OpenSSL	Vysoká	**7.5**
07.	Zraniteľnosť v module Host Engineering H2-ECOM100	Vysoká	**7.5**
08.	Dve zraniteľnosti v Mitsubishi Electric MELSEC iQ-F, GOT a Tension Controller	Vysoká	**7.5**
09.	Zraniteľnosť v National Instruments Corp CompactRIO	Vysoká	**7.5**

Národný bezpečnostný úrad
Budatínska 30
851 06 Bratislava

Mail: sk-cert@nbu.gov.sk
Mobil: +421 903 993 706
Tel: +421 2 6869 2915

SK-CERT
Naša značka:
01439/2020/SK-CERT-289

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero zraniteľností v produktoch Microsoft

Popis

Spoločnosť Microsoft vydala bezpečnostné aktualizácie na svoje portfólio produktov, ktoré opravujú viacero bezpečnostných zraniteľností.
Najzávažnejšia bezpečnostná zraniteľnosť nachádzajúca sa v produkte SharePoint spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému, autentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

11.12.2020

CVE

CVE-2020-16996, CVE-2020-17094, CVE-2020-17095, CVE-2020-17096, CVE-2020-17098, CVE-2020-17099, CVE-2020-17115, CVE-2020-17119, CVE-2020-17120, CVE-2020-17121, CVE-2020-17122, CVE-2020-17123, CVE-2020-17124, CVE-2020-17125, CVE-2020-17126, CVE-2020-17127, CVE-2020-17128, CVE-2020-17129, CVE-2020-17130, CVE-2020-17133, CVE-2020-17138, CVE-2020-17140, CVE-2020-17143, CVE-2020-17144, CVE-2020-17147, CVE-2020-17148, CVE-2020-17152, CVE-2020-17153, CVE-2020-17156, CVE-2020-17158, CVE-2020-17160

Zasiahnuté systémy

Microsoft Windows
Microsoft Edge (EdgeHTML-based)
Microsoft Edge for Android
ChakraCore
Microsoft Office and Microsoft Office Services and Web Apps
Microsoft Exchange Server
Azure DevOps
Microsoft Dynamics
Visual Studio
Azure SDK
Azure Sphere

Kompletný rozpis zasiahnutých systémov môžete nájsť na adrese https://support.microsoft.com/en-us/help/20201208/security-update-deployment-information-december-8-2020

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií
Neoprávnený prístup k citlivým údajom

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://msrc.microsoft.com/update-guide/releaseNote/2020-Dec https://support.microsoft.com/en-us/help/20201208/security-update-deployment-inpremation-december-8-2020

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti v Medtronic MyCareLink Smart Model 2500 Patient Reader

Popis

Spoločnosť Medtronic vyxala aktualizácie na svoj produkt MyCareLink Smart, ktorá opravuje tri bezpečnostné zraniteľnosti.
Najzávažnejšia bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje lokálnemu, neautentifikovanému útočníkovi prostredníctvom podvrhnutia špeciálne vytvoreného firmwaru vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

10.12.2020

CVE

CVE-2020-25183, CVE-2020-25187, CVE-2020-27252

Zasiahnuté systémy

Medtronic MyCareLink Smart Model 2500 Patient Reader verzia staršia ako 5.2

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsma-20-345-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti v platobných termináloch Verifone a Ingenico Telium

Popis

Spoločnosti Verifone a Ingenico vydali bezpečnostné aktualizácie na svoje platobné terminály Verifone VX a MX a Ingenico Telium 2.
Najzávažnejšia bezpečnostná zraniteľnosť umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať škodlivý kód s následkom úplného narušenia dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

23.10.2020

CVE

CVE-2018-17765, CVE-2018-17766, CVE-2018-17767, CVE-2018-17769, CVE-2018-17770, CVE-2018-17771, CVE-2018-17772, CVE-2019-14711, CVE-2019-14712, CVE-2019-14713, CVE-2019-14716, CVE-2019-14717, CVE-2019-14718, CVE-2019-14719

Zasiahnuté systémy

Ingenico Telium 2 SDK vo verzii staršej ako 9.32.03 patch N
Verifone Linux MX MX900 series Pinpad platobné terminály s OS 30251000
Verifone VerixV Pinpad platobné terminály s QT000530

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Eskalácia privilégií

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://www.cyberdlab.com/research-blog/posworld-vulnerabilities-within-ingenico-telium-2-and-verifone-vx-and-mx-series-point-of-sales-terminals

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 8.1
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Viacero zraniteľností v portfóliu produktov Siemens

Popis

Spoločnosť Siemens vydala bezpečnostné aktualizácie na svoje portfólio industriálnych systémov, ktoré opravujú veľké množstvo bezpečnostných zraniteľností.
Najzávažnejšia zraniteľnosť sa nachádza v produkte SICAM A8000, je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi vykonať neoprávnené zmeny v systéme a získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

08.12.2020

CVE

CVE-2017-12734, CVE-2017-12735, CVE-2018-4833, CVE-2019-10924, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-13946, CVE-2019-15126, CVE-2019-19283, CVE-2019-19284, CVE-2019-19285, CVE-2019-19286, CVE-2019-19287, CVE-2019-19288, CVE-2019-19289, CVE-2019-8460, CVE-2020-0543, CVE-2020-13988, CVE-2020-15791, CVE-2020-15796, CVE-2020-28214, CVE-2020-28396, CVE-2020-7565, CVE-2020-7566, CVE-2020-7567, CVE-2020-7568, CVE-2020-7580, CVE-2020-7581, CVE-2020-7585, CVE-2020-7586, CVE-2020-7587, CVE-2020-7588

Zasiahnuté systémy

Siemens SENTRON PAC3200: verzie 2.4.5 a staršie
Siemens SENTRON PAC4200: verzie 2.0.1 a staršie
SIRIUS 3RW5 komunikačný modul Modbus TCP: všetky verzie
Siemens XHQ Operations Intelligence
Siemens SICAM A8000 RTUs
Siemens SIMATIC Controller Web Servers
Siemens SIMATIC S7-300 and S7-400 CPUs (Aktualizácia C)
Siemens Industrial Products (Aktualizácia B)
Siemens SIMATIC, SIMOTICS (Aktualizácia A)
Siemens UMC Stack (Aktualizácia D)
Siemens SIMATIC, SINAMICS, SINEC, SINEMA, SINUMERIK (Aktualizácia D)
Siemens SIMATIC, SINAMICS (Aktualizácia B)
Siemens PROFINET-IO Stack (Aktualizácia C)
Siemens Industrial Products (Aktualizácia K)
Siemens LOGO! Soft Comfort (Aktualizácia A)
Siemens SCALANCE X Switches, RUGGEDCOM WiMAX, RFID 181-EIP, a SIMATIC RF182C (Aktualizácia D)
Siemens LOGO! (Aktualizácia A)

Kompletný zoznam zraniteľných zariadení nájdete na odkazoch v časti Zdroje.

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby
Neoprávnený prístup k citlivým údajom
Neoprávnený prístup do systému

Odporúčania
Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov. Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu. Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu alebo únik informácií, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje
https://us-cert.cisa.gov/ics/advisories/ICSA-17-243-02 https://us-cert.cisa.gov/ics/advisories/ICSA-18-165-01 https://us-cert.cisa.gov/ics/advisories/ICSA-19-134-03 https://us-cert.cisa.gov/ics/advisories/icsa-19-253-03 https://us-cert.cisa.gov/ics/advisories/icsa-20-042-04 https://us-cert.cisa.gov/ics/advisories/icsa-20-161-05 https://us-cert.cisa.gov/ics/advisories/icsa-20-161-04 https://us-cert.cisa.gov/ics/advisories/icsa-20-196-05 https://us-cert.cisa.gov/ics/advisories/icsa-20-224-05 https://us-cert.cisa.gov/ics/advisories/icsa-20-252-07 https://us-cert.cisa.gov/ics/advisories/icsa-20-252-02 https://us-cert.cisa.gov/ics/advisories/icsa-20-343-09 https://us-cert.cisa.gov/ics/advisories/icsa-20-343-07 https://us-cert.cisa.gov/ics/advisories/icsa-20-343-06 https://us-cert.cisa.gov/ics/advisories/icsa-20-343-05

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.8
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosti vo WECON LeviStudioU

Popis

Spoločnosť WECON Technology zverejnila informácie o bezpečnostnej zraniteľnosti svojho produktu LeviStudioU.
Najzávažnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje lokálnemu, autentifikovanému útočníkovi vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému.

Dátum prvého zverejnenia varovania

03.12.2020

CVE

CVE-2020-16243, CVE-2020-25186, CVE-2020-25199

Zasiahnuté systémy

WECON Technology LeviStudioU vo verzii 2019-09-21 (vrátane)

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Po odstránení zraniteľností, ktoré mohli spôsobiť vzdialené vykonanie kódu, je dobrou praxou kontrola systému a zmena všetkých hesiel a kľúčov na dotknutom systéme a aj na iných systémoch, kde sa používalo rovnaké heslo či kľúč.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-238-03

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v OpenSSL

Popis

Vývojári knižnice OpenSSL vydali bezpečnostnú aktualizáciu, ktorá opravuje bezpečnostnú zraniteľnosť. Zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.12.2020

CVE

CVE-2020-1971

Zasiahnuté systémy

OpenSSL 1.1.1 vo verzii staršej ako 1.1.1i
OpenSSL 1.0.2 vo verzii staršej ako 1.0.2x

Následky

Zneprístupnenie služby

Odporúčania

Odporúčame uistiť sa, či Vaše produkty a služby nevyužívajú predmetnú knižnicu v zraniteľnej verzii. V prípade, že áno, administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.openssl.org/news/secadv/20201208.txt
https://nvd.nist.gov/vuln/detail/CVE-2020-1971

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v module Host Engineering H2-ECOM100

Popis

Spoločnosť Host Engineering vydala bezpečnostnú aktualizáciu pre svoj ethernetový modul Host Engineering H2-ECOM100, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočným overovaním používateľských vstupov umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

10.12.2020

CVE

CVE-2020-25195

Zasiahnuté systémy

H0-ECOM100 Module vo verzii 6x (všetky verzie) s firmvérom starším ako 4.0.348 (vrátane)
H0-ECOM100 Module vo verzii 7x s firmvérom starším ako 4.1.113 (vrátane)
H0-ECOM100 Module vo verzii 9x s firmvérom starším ako 5.0.149 (vrátane)
H2-ECOM100 Module vo verzii 5x (vrátane) s firmvérom starším ako 4.0.2148 (vrátane)
H2-ECOM100 Module vo verzii 8x s firmvérom starším ako 5.0.1043 (vrátane)
H4-ECOM100 Module: Firmware Versions 4.0.2148 (vrátane)

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-345-02

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Dve zraniteľnosti v Mitsubishi Electric MELSEC iQ-F, GOT a Tension Controller

Popis

Spoločnosť Mitsubishi Electric vydala bezpečnostné aktualizácie na svoje produkty MELSEC iQ-F, GOT a Tension Controller, ktoré opravujú dve bezpečnostné zraniteľnosti.
Najzávažnejšia zraniteľnosť sa nachádza v produktoch GOT a Tension Controller a umožňuje vzdialenému, neautentifikovanému útočníkovi prostredníctvom zaslania špeciálne vytvoreného paketu spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

08.12.2020

CVE

CVE-2020-5665, CVE-2020-5675

Zasiahnuté systémy

Mitsubishi Electric FX5U(C) CPU module firmware vo verzii staršej ako 1.061
Mitsubishi Electric GOT2000 series, model GT21 GT2107-WTBD všetky verzie
Mitsubishi Electric GOT2000 series, model GT21 GT2107-WTSD všetky verzie
Mitsubishi Electric GOT2000 series, model GT21 GT2104-RTBD všetky verzie
Mitsubishi Electric GOT2000 series, model GT21 GT2104-PMBD všetky verzie
Mitsubishi Electric GOT2000 series, model GT21 GT2103-PMBD všetky verzie
Mitsubishi Electric GOT SIMPLE series, model GS21 GS2110-WTBD všetky verzie
Mitsubishi Electric GOT SIMPLE series, model GS21 GS2107-WTBD všetky verzie
Mitsubishi Electric Tension Controller LE7-40GU-L všetky verzie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom a používateľom odporúčame vykonať aktualizáciu zasiahnutých systémov.
V prípade Mitsubishi Electric GOT a Tension Controllera administrátorom odporúčame sledovať stránku výrobcu a po vydaní bezpečnostných záplat vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-343-02
https://us-cert.cisa.gov/ics/advisories/icsa-20-345-01

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre:** 7.5
Klasifikácia	☒ **Neutajované / TLP(WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Zraniteľnosť v National Instruments Corp CompactRIO

Popis

Spoločnosť National Instruments Corp vydala bezpečnostnú aktualizáciu pre svoj produkt CompactRIO, ktorá opravuje bezpečnostnú zraniteľnosť.
Bezpečnostná zraniteľnosť je spôsobená nedostatočnou implementáciou bezpečnostných mechanizmov a umožňuje vzdialenému, neautentifikovanému útočníkovi spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

03.12.2020

CVE

CVE-2020-25191

Zasiahnuté systémy

CompactRIO driver vo verzii staršej ako 20.5

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.
Riadiace jednotky a systémy odporúčame prevádzkovať úplne oddelené od internetu.

Zdroje

https://us-cert.cisa.gov/ics/advisories/icsa-20-338-01